PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-249264
(43)Date of publication of application : 26.09.1995

(51)Int.Cl. G11B 20/10
G06F 12/14

(21)Application number : 06-065426 (71)Applicant : INTEC:KK
BROTHER IND LTD
(22)Date of filing : 10.03.1994 (72)Inventor : KAWASAKI TETSUO
HOSHIBA SHINJI
TANIGUCHI TOSHINORI

(54) RECORDING SYSTEM AND RECORDING/REPRODUCING SYSTEM FOR CD-ROMAND CD-ROM DISK

(57)Abstract:
PURPOSE: To unnecessitate control of key information for deciphering ciphered data recorded in a CD-ROM disk.
CONSTITUTION: When desired information is ciphered and recorded in the CD- ROM disk 1key information required for decoding this ciphered information is recorded in a proper region 3 in the CD-ROM disk 1 with the ciphering information. When recorded contents of the CD-ROM disk 1 in which ciphering information is recorded by this recording system are reproduceda desired key information is read out from the same CD-ROM disk 1 with ciphering informationand the ciphered information can be deciphered by only this read-out information.

CLAIMS

[Claim(s)]
[Claim 1]In a recording method of CD-ROM for enciphering necessary information and recording on a CD-ROM discA recording method of CD-ROM recording key information required to decrypt encipherment information which should be recorded on a CD-ROM disc in this CD-ROM disc with this encipherment information.

[Claim 2]In a play back system of CD-ROM for enciphering necessary informationrecording on a CD-ROM discreading this recorded encipherment information from a CD-ROM discand decrypting itKey information required to decrypt encipherment information which should be recorded on a CD-ROM disc is recorded in this CD-ROM disc with this encipherment informationA play back system of CD-ROM decrypting this encipherment information using key information which read encipherment information and key information which are recorded in a CD-ROM disc at the time of playbackand was read from a CD-ROM disc.
[Claim 3]A CD-ROM discwherein key information which needs necessary information to decode recorded encipherment information in a CD-ROM disc currently enciphered and recorded is recorded in this CD-ROM disc.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Industrial Application]This invention records the enciphered variety of information on a CD-ROM discand relates to the recording method of CD-ROM for playingthe play back system of CD-ROMand a CD-ROM disc.
[0002]
[Description of the Prior Art]In order to record a lot of informationthe optical play back system using a laser beam etc. is publicly knownand especially compact disk read-only memory and what is called a CD-ROM disc are widely used as an optical disc for it not only in the field of an audio but in various kinds of fields. Although the CD-ROM disc has generally been used as an only for [playback] type recording mediuman added-a postscript type thing is also developed in recent yearsand it is **(ed) by practical use.
[0003]by the wayan only for [playback] type -- be -- the added type of a postscript -- be -- for the security protection of the information written in a CD-ROM discthe information which should be recorded is enciphered and the demand of recording this enciphered information on a CD-ROM disc often arises. As one art of filling such a demandfor example as explained in the 4th page top left column of JPS64-91256APerform scramble processing which added code data when making an user datum record on a CD-ROM discmake it encryption dataand it is made to recordAfter performing descrambling processing for encryption data with a CD-ROM driverThe art which outputs decode data (the same as that of code data) and encryption data to a computer after performing exclusion logic treatmentand enabled it to perform security of an user datum certainly by this with an interface is publicly known. Since this conventional

technology is composition which carries out decoding processing of the necessary information using hardwareit has the big feature at the point that the time of processing can be substantially shortened compared with the case where processing is used with software.
[0004]
[Problem(s) to be Solved by the Invention]Howeveraccording to the conventional technology mentioned abovesince the key and hardware for decryption are related closelywhen change of a key is requiredchange of hardware or a change of decoding RAM contents must be madeand cost considerable for change of a key is needed. Thereforethe tendency which continues using a fixed key is produced and it has the problem of bringing a result which closes acquiring a cue for a third party to decode the contents of record of a CD-ROM disc if comparatively easy. Since the format of the data which this should record on a CD-ROM disc is standardized by ISO9660It is based on a Reason that the key for decryption of the data content of the address with which the specific contents defined by the standard are stored if the same key is continued and used at a cue can be guessed comparatively easily. And once it does in this way and the key for decryption becomes known to a third partythe fault that the contents of record of the remaining CD-ROM discs will also be decoded promptly will be produced.
[0005]Other problems by the above-mentioned conventional technology are that management of a key is needed separately and the cost for key information management occurs in order to have to manage the contents of the key for decryption by a proper meansfor examplethe means of indicating to a code bookbeforehand. This problem is a problem generally producedwhen it is going to record encryption data not only on the above-mentioned conventional technology but on a CD-ROM disc.
[0006]the purpose of this invention -- one [therefore] of the above-mentioned problem in conventional technologyfaultsetc. -- again -- yes -- shoes -- or it is in providing the recording method of CD-ROM which can improve allthe play back system of CD-ROMand a CD-ROM disc.
[0007]It will be as follows if the purposes of this invention are more concretely enumerated in illustration.
[0008]Provide the recording method of CD-ROM and the play back system of CD-ROM which made unnecessary management of the key information accompanying change of the key for encryption of the information which should be recorded on a CD-ROM disc.
[0009]Provide the CD-ROM disc which made unnecessary management of the key information for the decipherment of the recorded encryption data.
[0010]Provide the recording method of CD-ROM and the play back system of CD-ROM which enabled it to use several different keyswithout raising cost so that a third party cannot know easily the key for the decipherment of the data

content enciphered and recorded.
[0011]A key required in order to decrypt the information as which the information which should be recorded on a CD-ROM disc was enciphered and enciphered can be **(ed) by changing easily for every recording mediumAnd provide the recording method of CD-ROM which enabled it to make management of a key unnecessarythe play back system of CD-ROMand a CD-ROM disc.
[0012]
[Means for Solving the Problem]In a recording method of CD-ROM for this invention enciphering necessary information and recording on a CD-ROM disc which is an optical discin order to solve an aforementioned problemIt is characterized by recording key information required to decrypt encipherment information which should be recorded on a CD-ROM disc in this CD-ROM disc with this encipherment information.
[0013]In a play back system of CD-ROM for this invention enciphering necessary information and recording it on a CD-ROM discand reading this recorded encipherment information from a CD-ROM discand decrypting itKey information required to decrypt encipherment information which should be recorded on a CD-ROM disc is recorded in this CD-ROM disc with this encipherment informationIt is characterized by decrypting this encipherment information using key information which read encipherment information and key information which are recorded in a CD-ROM disc at the time of playbackand was read from a CD-ROM disc.
[0014]This invention is characterized by recording key information which needs necessary information to decode recorded encipherment information in a CD-ROM disc currently enciphered and recorded in this CD-ROM disc.
[0015]
[Function]When enciphering necessary information and recording in a CD-ROM diskey information required in order to decrypt the encipherment information read from this CD-ROM disc after that is also recorded in that CD-ROM disc. Therebyencipherment information and key information required for this decipherment are always manageable to one.
[0016]In playing the contents of record of the CD-ROM disc on which encipherment information is recorded by such a recording methodNecessary key information is read from the same CD-ROM disc with encipherment informationand necessary decryption is performedwithout being able to decrypt encipherment information and being conscious of especially the key information for decryption only using these read-out information.
[0017]Thuseven if it changes key information suitablyin the CD-ROM diskey information required for decryption of the encipherment information currently recordedi.e.a decipherment is always recordedand management of only key information is unnecessary.

[0018]
[Example]Hereafterwith reference to Drawingsit explains to details per working example of this invention.
[0019]The CD-ROM recording system for recording necessary information on a CD-ROM disc by this invention and the CD-ROM reproducing system which makes this and a pair and constitutes CD-ROM record and a reproducing system are shown in drawing 1 and drawing 2respectively.
[0020]Firstif the CD-ROM recording system 10 is explained with reference to drawing 1Memory storage with which the user datum which should record 11 on CD-ROM disc 1 is stored beforehandA keyboard for 12 to input various command data and 13 are the read-out control sections for reading it one by oneas the necessary user datum directed by the keyboard 12 is later mentioned from the memory storage 11The necessary user datum read by the read-out control section 13 is sent to the encrypted unit 14.
[0021]The recording method for recording a desired user datum on CD-ROM disc 1 in advance of the explanation about the encrypted unit 14 is explained with reference to drawing 3.
[0022]as shown in drawing 3the record section of CD-ROM disc 1 is divided roughly into the pre-gap field 2 and the ISO9660 field 4 -- ISO9660 field -- many sectors S1S2and S3 ... is set up. these sectors S1S2and S3 ... is constituted according to the data format based on JISX0606-1990 about BORYUUMU of CD-ROM for ISO9660 information exchange and the structure of a file which were published in 1988. [and]
[0023]Thereforedivide the data which should be recorded into 2048 bytes of user data area established in each sectorand it is stored one by oneSince contents of the data for one sector which should be recorded on CD-ROM disc land a preparation method for the same are explained by the standard in full detailHereexplaining the details omits and a necessary user datum is only stopped to explain only the point that every 2048 bytes are divided and recorded on the sector of the ISO9660 field 4. In the ISO9660 field 4a free space can be appointed by the definition of a data formatand it is used as the cryptographic key recording sector 3 of this example.
[0024]If it returns to drawing 1the keyboard 12 has the function to input the encryption sector information which shows whether the user datum recorded on which sector should be encipheredwhen carrying out division recording of the user datum to a sectorin order to record a further necessary user datum on CD-ROM disc 1. This encryption sector information is sent to the cryptographic key generation part 15 in the encrypted unit 14 from the keyboard 12.
[0025]Based on the encryption sector information sent from the keyboard 12the cryptographic key generation part 15The peculiar cryptographic key to the sector which should encipher and record an user datum is generated for every

necessary sectorand it has a function which cryptographic key information and the number information of the sector for which the cryptographic key is used create two or more sets of cryptographic key data which became a groupand is held.
[0026]These cryptographic key data is sent to the CD-ROM mastering device 18 to the timing which records the cryptographic key recording sector 3and these cryptographic key data is recorded on the cryptographic key recording sector 3 in CD-ROM disc 1 by the CD-ROM mastering device 18 (refer to drawing 3).
[0027]On the other handthe read-out control section 13 begins to read at a time one sector of necessary user data stored in the memory storage 11and sends them to the encryption section 16 of the encrypted unit 14. If the encryption section 16 can be constituted using commercial encryption IC and the user datum for one sector is received from the read-out control section 13it will output the cryptographic key requirement signal required as sending the cryptographic key to this sector to the encryption section 16 to the cryptographic key generation part 15. When the cryptographic key generation part 15 answers this cryptographic key requirement signal and the cryptographic key is prepared to that sectorThat iswhen it is ordered from the keyboard 12 that the user datum which should be recorded on the sector should be encipheredthe cryptographic key currently beforehand prepared for the sector is sent to the encryption section 16. When the sector is not ordered encryption and the cryptographic key is not prepared [therefore]transmission of the data from the cryptographic key generation part 15 to the encryption section 16 is not performed.
[0028]Thereforein the encryption section 16the user datum sent at a time one sector from the read-out control section 13 is receivedEncryption enciphers using the cryptographic key supplied from the cryptographic key generation part 15 only about the thing of the sector currently orderedand sends the user datum for one enciphered sector to the interface part 17. The user datum which encryption should record on the sector which is not ordered on the other hand is sent to the interface control part 17 as it iswithout being enciphered.
[0029]The user datum for every sector which did in this wayand was enciphered or is not enciphered in the interface control part 17 is sent to the CD-ROM mastering device 18 one by oneThe user datum for every sectors of these is recorded one by one on the sector S1 provided in the ISO9660 field 4 of CD-ROM disc 1S2and ... by the predetermined procedure. drawing 3 shows in this example -- as -- the sector S1S2S7and S9 -- the user datum currently recorded on ... is not enciphered -- the sector S3S6and S8 -- the user datum currently recorded on ... is enciphered. Sector S4 and S5 are defined as a free spaceand are used as a sector which records a cryptographic key. Howeverit is not limited to the thing of this one working example of which sector an user datum

is enciphered and on which free space a cryptographic key is recordedbut it can be set up suitably. The sector which should be enciphered [should be replaced with and] and recorded on ordering each time from the keyboard 12 may be fixed like until [from the 1st / 200th].
[0030]Anywayan user datum is enciphered by the predetermined field in CD-ROM disc 1Or it has the feature at the point currently recorded on the predetermined field in same CD-ROM disc 1 as it that a cryptographic key required to decrypt the user datum which was recorded as sector informationwithout being enciphered and was recorded by doing in this way on the other hand is big. One of the advantages by this feature is that management of a cryptographic key becomes unnecessary.
When playing and decrypting the encryption data recorded especially on CD-ROM disc 1it is not giving cryptographic key information separately from the outside.

[0031]Although the cryptographic key was made into another thing for every sector in above-mentioned working exampleof coursethe cryptographic key of all the encryption sectors may be made the same. even if it uses many cryptographic keyssince it is not generatedif a cryptographic key is changed for every sectorthe troublesomeness of cryptographic key management makes difficult the decipherment of the user datum by a third partywithout raising the cost of cryptographic key managementcan boil security protection capability markedly and can raise it.
[0032]Nextthe CD-ROM reproducing system 20 for playing and decrypting the user datum which enciphered to CD-ROM disc 1 with the CD-ROM recording system 10 of drawing 1and was recorded with reference to drawing 2 is explained.
[0033]The CD-ROM reproducing system 20 has the CD-ROM drive device 21 for reading the contents of record of CD-ROM disc 1. By setting CD-ROM disc 1 in the CD-ROM drive device 21the cryptographic key data currently recorded on the cryptographic key recording sector 3 of CD-ROM disc 1 is read firstand is sent to the interface control part 22. And the read cryptographic key data is stored in the memory 25 in the decoding unit 23.
[0034]After an appropriate timeunder control of the interface control part 22the first one sector (S1) currently recorded on the ISO9660 field 4 in CD-ROM disc 1 is read by the CD-ROM drive device 21and is sent via the interface control part 22 at the decoding section 24. The decoding section 24 can also be constituted using commercial decryption IC. The decoding section 24 requires read-out of the cryptographic key corresponding to this sector S1 from the memory 25.
[0035]In this examplesince the sector S1 is not an encryption sectorin the memory 25the cryptographic key corresponding to the sector S1 is not stored.

Thereforeany cryptographic key information from the memory 25 is not outputtedbut the user datum currently recorded in the sector S1 is outputted from the decoding section 24 as it isand is stored in the buffer memory 26. The user datum currently recorded on the sector S2 is completely processed similarly.

[0036]If the contents of record of the sector S3 are inputted into the decoding section 24a cryptographic key required to decrypt the encryption user datum currently recorded on the sector S3 will be chosen considering the number information in cryptographic key data as a cueand a necessary cryptographic key will be sent to the decoding section 24 from the memory 25. In the decoding section 24decoding processing of the encryption user datum currently recorded on the sector S3 using this cryptographic key is performedand the decrypted user datum is sent to the buffer memory 26.

[0037]the sector S1 and S2 -- what was enciphered among the user data currently recorded on ... will be ******(ed) by the cryptographic key supplied from the memory 25and will be sent to the buffer memory 26. [thus] On the other handthe user datum which was not enciphered passes the decoding unit 23 as it isand is stored in the buffer memory 26. Thereforethe necessary user datumi.e.the decrypted user datumbefore carrying out encryption can be taken out from the buffer memory 26. Although the cryptographic key is recorded on sector S4 and S5it is a data format top free spaceand extraction of an user datum is not influenced.

[0038]The effect like the next is expected at least by using the system shown in drawing 1 and drawing 2.

[0039]Since it is recorded together in CD-ROM disc 1 which records the user datum as which the cryptographic key used for enciphering an user datum was encipheredit is not necessary to manage the key information on encryption separately. Thereforethe cost for management of a cryptographic key is released from the troublesomeness of being not only unnecessary but its management.

[0040]Since an encryption user datum and a cryptographic key are recorded in same CD-ROM disc 1Since what is necessary is just not to record this change separately and to read a cryptographic key required for decryption from that CD-ROM disc 1 at the time of playbackeven if it changes a cryptographic key howthe time and effort which decryption takes is simplified remarkably.

[0041]CD-ROM disc 1 to which encryption record of the user datum was performed by this methodSince cryptographic key information is recordedthere is no concept of management of the cryptographic key information corresponding to CD-ROM disc 1cryptographic key information management completely becomes unnecessaryand playback of an user datum and decryption can be performedwithout being completely conscious of encryption.

[0042]Thussince the management cost of cryptographic key information does not pose a problem at alleven if it uses cryptographic keys differentfor example for every CD-ROM discany cost is not generatedand the security protection of record can be raised remarkablywithout producing cost. Naturally this corresponds also about the composition of this example which changes a cryptographic key for every sector about one CD-ROM disc 1and the code record in which a third party's decipherment is very difficult is possible for it at low cost.
[0043]Nextwith reference to drawing 4 thru/or drawing 6by performing a predetermined recording control program and reproduction control program in a computer system explains other working example which was made to perform record of CD-ROM disc 1and playback like the case of above-mentioned working example.
[0044]Drawing 4 enciphers and records the user datum stored in the external storage 31 on CD-ROM disc 1and. It is an outline lineblock diagram of the CD-ROM record and the reproducing system 30 by this invention using the computer system for reading the user datum currently enciphered and recorded from CD-ROM disc 1and playing.
[0045]The CD-ROM mastering device 18 and the CD-ROM drive device 21 are the same as each device shown in drawing 1 and drawing 2 at drawing 4and these devices 18 and 21 and outboard recorders 31 are connected to the computer system 32. A keyboard is shown by the numerals 38.
[0046]This computer system 32 is the publicly known composition that it is connected mutually and the central processing unit (CPU) 33the random access memory (RAM) 34the read-only memory (ROM) 35and the input/output interface device (I/F) 36 change by bus 37. And by executing the recording control program and reproduction control program which are stored in ROM35 in CPU33Record of the encryption user datum to CD-ROM disc 1 and playback of the encryption user datum recorded by doing in this wayand decryption are performed like the case of composition of having been shown in drawing 1 and drawing 2.
[0047]Firstthe recording operation by CD-ROM record and the reproducing system 30 is explainedreferring to drawing 5.
[0048]A start of execution of a recording control program will determine an encryption target sector according to the data in which the encryption target sector inputted from the keyboard 38 is shown at Step 41 first. In the following step 42the cryptographic key of each sector to be enciphered is generated and the generated cryptographic key is stored in RAM34 as cryptographic key data. This cryptographic key data is the same as that of what was explained based on drawing 1.
[0049]In Step 43it is distinguished whether the CD-ROM mastering device 18 is

a writing state to the cryptographic key recording sector 3. If the CD-ROM mastering device 18 is a writing state to the cryptographic key recording sector 3the discriminated result of Step 43 will serve as YESand will progress to Step 44. In Step 44the cryptographic key data stored in RAM34 is sent to the CD-ROM mastering device 18 via CPU33 and I/F36Cryptographic key data is recorded on the cryptographic key recording sector 3 of CD-ROM disc 1 set in the CD-ROM mastering device 18. The end check of whether all necessary user data were recorded at Step 49 after an appropriate time is performedand when all records have not been completed yetit returns to Step 43.

[0050]When record of cryptographic key data is completedthe discriminated result of Step 43 serves as NOand in Step 45the user datum for one sector is read from the external storage 31. In the following step 46it is distinguished whether the sector which should record the user datum for this one read sector is an encryption target sector. The discriminated result of Step 46 becomes that the sector which should record the user datum for the one sector is an encryption target sector with YESand it goes into Step 47.

[0051]In Step 47processing for enciphering the user datum for one sector using the cryptographic key for the sector among the cryptographic keys generated at Step 42 is performedand the user datum for one sector by which encryption processing was carried out at the following step 48 is sent to the CD-ROM mastering device 18. The CD-ROM mastering device 18 records the user datum for one received sector on a necessary sector.

[0052]Since Step 47 is not performed when the discriminated result of Step 46 is NOencryption processing is not carried outbut the user datum for one sector read from the external storage 31 is sent to the CD-ROM mastering device 18 as it isand is recorded on a necessary sector.

[0053]Thusif all user data are written in CD-ROM disc 1the discriminated result of Step 49 will serve as YESand execution of a recording control program will be completed.

[0054]Nextplayback of the CD-ROM record and the reproducing system 30 for reading the data which did in this way and was recorded on CD-ROM disc 1 from CD-ROM disc 1and playingand decryption operation are explainedreferring to drawing 6.

[0055]In Step 51it is first distinguished after the execution start of a reproduction control program whether it is the exchange whereabouts no of CD-ROM disc 1. In with exchangeit progresses at Step 52and the cryptographic key data currently recorded on the cryptographic key recording sector 3 is readand it progresses to Step 53 here. Since reading of cryptographic key data is already made when the discriminated result of Step 51 is NOStep 52 is not performed but goes into Step 53.

[0056]In Step 53the data for one sector is read from CD-ROM disc 1 with the

CD-ROM drive device 21and it is distinguished whether this read data for one sector is data of a decryption target sector at Step 54. It goes that it is a decryption target sector into Step 55necessary decoding processing is performed using the cryptographic key data corresponding to the sector of the cryptographic key data already read at Step 52and it progresses to Step 56. On the other handwhen the data for one sector read at Step 53 is not data of a decryption target sectorit goes into Step 56without performing Step 55.
[0057]In Step 56it is distinguished whether reading of all the required sectors was completedand when no reading of required sectors is still completedit returns to Step 53. Thusthe data recorded on CD-ROM disc 1 is read for every sectorand decoding processing is performed only about the required sector of decryption. After reading of all the required sectors is completedthe discriminated result in Step 56 serves as YESand execution of a reproduction control program is completed. Thusthe user datum recorded on CD-ROM disc 1 can be played and decrypted.
[0058]The CD-ROM record and the reproducing system 30 shown in drawing 4 also have the same advantage as the case of the system shown in drawing 1 and drawing 2.
[0059]
[Effect of the Invention]The effect by this invention is as follows.
[0060]Since it is recorded in the CD-ROM disc which records the data in which the cryptographic key information used for enciphering the data which should be recorded on a CD-ROM disc was encipheredit is not necessary to manage cryptographic key information separately. Thereforethe cost for management of cryptographic key information is released from the troublesomeness of being not only unnecessary but its management.
[0061]Since encryption data and cryptographic key information are recorded into the same CD-ROM discEven if it changes a cryptographic key howthe information about this change is recorded separatelySince what is necessary is just not to manage and to read a cryptographic key required for decryption from the CD-ROM disc at the time of playback of the data in a CD-ROM discthe time and effort which decryption takes is simplified remarkably.
[0062]By performing encryption record of data by the method of this inventionencryption data and the cryptographic key information for decoding this the CD-ROM disc currently recorded togetherThere is no concept of management of the cryptographic key information corresponding to a CD-ROM discall cryptographic key information management becomes needlessnessthe management cost can be made unnecessaryand also playback of an user datum and decryption can be performedwithout being completely conscious of encryption.
[0063]Since the management cost of cryptographic key information does not pose a problem at alleven if it uses cryptographic keys differentfor example for

every CD-ROM discany management cost is not generatedand the security protection of record can be raised remarkablywithout producing cost.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]The lineblock diagram showing one working example of the recording system of the CD-ROM disc by this invention.

[Drawing 2]The lineblock diagram showing one working example of the CD-ROM disc reproducing system by this invention.

[Drawing 3]The explanatory view of the record section in the CD-ROM disc for explaining the recording method of the CD-ROM disc used in the system of drawing 1 and drawing 2.

[Drawing 4]The lineblock diagram showing other working example of the CD-ROM disc record and the reproducing system by this invention.

[Drawing 5]The flow chart which shows the recording control program executed in the computer system of drawing 4.

[Drawing 6]The flow chart which shows the reproduction control program executed in the computer system of drawing 4.

[Description of Notations]

1 CD-ROM disc
3 Cryptographic key recording sector
4 ISO9660 field
10 CD-ROM recording system
11 Memory storage
14 Encrypted unit
15 Cryptographic key generation part
16 Encryption section
20 CD-ROM reproducing system
23 Decryption YUNYUTTO
24 Decoding section
30 CD-ROM record and a reproducing system
S1 thru/or S9 Sector